REMARKS

Claims 1, 4-9 and 11-22 are pending. In the Final Office Action, Claims 1, 4-9 and 11-22 were rejected under 35 U.S.C. §103(a) as being obvious over U.S. Publ. No. 2004/0250069 A1 to Kosamo in view of IEEE Standard 802.16-2001 ("IEEE Std" herein).

In the Response to Argument section, the Examiner asserts that "the feature of completing the service specific encryption process (including all necessary steps of message exchange) prior to establishing the traffic connection with the base station [...] is necessitated in order to enable a secure communication as understood by [a person of] ordinary skill in the art and also indicated by Kosamo (Fig 2, para 0043-0047)." (Final Office Action, page 10, emphasis supplied.)

On the contrary, the method of a subscriber station requesting and receiving a service-specific traffic encryption key from a base station of the present invention is not necessitated in order to enable a secure communication. Rather, the secure communication can be provided in numerous ways, and none of the cited ¶¶ 0043-0047 or Fig. 2 of Kosamo discloses or suggests that after *determining a service type for a traffic encryption key to be used for security on a traffic connection to the base station prior to establishing the traffic connection with the base station*, and *generating a Key Request Message for requesting a traffic encryption key corresponding to the determined service type..., wherein the Key Request message includes the determined service type*, as recited in Claim 1 and similarly recited in Claims 6, 13, 17 and 20.

The cited paragraphs 0043-0047 of Kosamo simply discuss generic encryption options, and fail to disclose or suggest such recitations of Claim 1. The cited Fig. 2 of Kosamo is also deficient, and simply provides a flow diagram without any indication of whether the *Key Request message includes the determined service type*.

Cited paragraphs 0043-0047 and Fig. 2 of Kosamo teach that a subscriber database entity (HSS) transfers encryption options for the subscriber, which is previously stored in the HSS according to the subscriber's selection, to a base station when the HSS receives a request for a call establishment from the subscriber terminal. The base station activates the encryption options transferred from the HSS and after the activation, data communication between the subscriber terminal and a destination is performed via the base station.

In contrast, in the present invention, a subscriber station requests a traffic encryption key corresponding to a service type previously determined by the subscriber from a base station prior to establishing the traffic connection with the base station, the subscriber station receives the traffic encryption key for the service type from the base station and after receiving the traffic encryption, the traffic connection with the base station is established.

As described above, Kosamo only teaches that the HSS transfers the encryption options to the base station and the base station activates the encryption option. Therefore, none of cited paragraphs 0043-0047 or Fig 2. of Kosamo discloses or suggests "receiving a Key Reply message including the traffic encryption key corresponding to the determined service type from the base station prior to establishing the traffic connection with the base station", as recited in Claim 1 and similarly recited in Claims 6, 13, 17 and 20.

In regards to the Examiner's allegation that such recitation is <u>necessitated</u> in order to enable a secure communication, the Examiner has failed to make the required showing of such necessary (i.e. inherent) operation. See MPEP 2112, "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" citing *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). Nowhere does the Examiner explain why it is believed that it is necessary to, after *determining a service type for a traffic encryption key to be used for security on a traffic connection to the base station prior to establishing the traffic connection with the base station*, request *a traffic encryption key corresponding to the determined service type ..., wherein the Key Request message includes the determined service type*, of the present invention.

Neither Kosamo nor the IEEE Std includes such disclosure or teaching, and for at least the above reasons, the rejection of Claims 1, 6, 13, 17 and 20 must be withdrawn. Without conceding patentability *per se*, dependent Claims 4-5, 7-9, 11-12, 14-16, 18, 19, 21 and 22 are allowable at least in view of their respective dependency therefrom.

Therefore, in view of the amendments and remarks herein, the currently pending claims are believed to represent a patentable departure from the cited art and are in condition for allowance. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, it is requested that the Examiner contact Applicants' attorney at the number given below.

Respectfully submitted,

Paul J. Farrell
Reg. No. 33,494
Attorney for Applicant(s)

THE FARRELL LAW FIRM, PC
290 Broadhollow Road, Suite 210E
Melville, New York 11747
Tel: (516) 228-3565